Optimal unambiguous state discrimination of two density matrices: A second class of exact solutions

Philippe Raynal[1] and Norbert Lütkenhaus[1,2]
[1] *Quantum Information Theory Group, Institut für Theoretische Physik I, and Max-Plank-Forschungsgruppe, Institut für Optik, Information und Photonik Universität Erlangen-Nürnberg, Staudtstr. 7, D-91058 Erlangen, Germany and*
[2] *Institute of Quantum Computing and Department of Physics and Astronomy University of Waterloo, Waterloo, Ontario, N2L 3G1, Canada*
(Dated: February 5, 2007)

We consider the Unambiguous State Discrimination (USD) of two mixed quantum states. We study the rank and the spectrum of the elements of an optimal USD measurement. This naturally leads to a partial fourth reduction theorem. This theorem shows that either the failure probability equals its overall lower bound given in term of the fidelity or a two dimensional subspace can be split off from the original Hilbert space. We then use this partial reduction theorem to derive the optimal solution for any two Geometrically Uniform (GU) states ρ_0 and $\rho_1 = U\rho_0 U^\dagger$, $U^2 = \mathbb{1}$, in a four dimensional Hilbert space. This represents a second class of analytical solutions for USD problems that cannot be reduced to some pure state cases. We apply our result to answer two questions that are relevant in implementations of the Bennett and Brassard 1984 quantum key distribution protocol using weak coherent states.

I. INTRODUCTION

Quantum State Discrimination is a crucial task in Quantum Information Theory, especially in a communication context. Whenever the signal states are non-orthogonal quantum states, perfect discrimination becomes impossible and one has to resort to various discrimination strategies. One might, for example, consider an error-free discrimination of the states. In that case, due to the non-orthogonality of the signal states, the measurement will sometimes fail to identify conclusively the signal. The goal therefore is to minimize the probability of inconclusive result, the so-called failure probability. This strategy is known as *Unambiguous State Discrimination* (USD).

The problem of unambiguously discriminating pure states with equal *a priori* probabilities was solved by Dieks [1], Ivanovic [2] and Peres [3]. Later Jaeger and Shimony presented the general solution for two pure states with arbitrary *a priori* probabilities [4]. Shortly after this result, Chefles proved that only linearly independent pure states can be unambiguously discriminated [5]. Chefles and Barnett then provided the optimal failure probability and its corresponding optimal measurement for n symmetric states [6]. Finally Sun *et al* [7] showed that the unambiguous discrimination of pure states is a convex optimization problem [8, 9, 10]. This result was later extended to mixed states by Eldar [11]. With respect to USD of mixed states, three reduction theorems related to simple geometrical considerations were developed [12, 13, 14]. They allow to reduce USD problems to simpler ones where a solution might be known. Important examples of such reducible problems are *Unambiguous State Discrimination of two mixed states with one-dimensional kernel* [15], *Unambiguous Comparison of two pure states* [16, 17, 18], *Unambiguous Comparison of n pure states with equal a priori probabilities and equal and real overlaps* [13], *State Filtering* [19, 20, 21] and *Unambiguous Discrimination of two subspaces* [22]. The three reduction theorems also define a *standard* form of USD problems. Such a standard form corresponds to the unambiguous discrimination of two density matrices of rank r in a $2r$-dimensional Hilbert space without trivial orthogonal subspaces and without block diagonal structure [12, 13, 14]. When a USD problem is not of that form, it can immediately be reduced to simpler ones. Later, necessary and sufficient conditions for a USD measurement to be optimal were derived by Eldar [23]. In addition lower and upper bounds on the failure probability were provided [15, 24]. Recently the lower bound was refined and a first class of exact solutions was found [14]. This class corresponds to pairs of mixed states such that the lower bound on the failure probability can be reached.

In this paper we first study the rank of the elements of an optimal USD measurement. We provide a theorem that reveals constraints on the rank of the elements associated to a conclusive detection. If we consider two density matrices ρ_0 and ρ_1 together with their respective *a priori* probabilities η_0 and η_1, these constraints depend on the positivity of the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. Note that the positivity of these two operators was already introduced in [14] as necessary and sufficient condition for the failure probability to reach the overall lower bound $2\sqrt{\eta_0\eta_1}\mathrm{Tr}(\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}})$.

A corollary to our first theorem can be derived assuming a standard USD problem. If the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$ are not positive semi-definite, then a two-dimensional subspace can

be split off from the original USD problem. This corollary actually is a fourth but incomplete reduction theorem. 'Reduction theorem' because no optimization is required onto that two-dimensional subspace. 'Incomplete' because the existence and the structure of this subspace are known but no complete analytical characterization is available yet.

The main result of the present paper is a consequence of our first theorem. We give a second class of exact solutions for generic USD problems. This class corresponds to any pair of Geometrically Uniform (GU) states in four dimensions. Two GU states are two unitary similar density matrices ρ_0 and $\rho_1 = U\rho_0 U^\dagger$ where the unitary matrix U is an involution i.e. $U^2 = \mathbb{1}$. We find that only three options exist depending on the spectrum of some operators. For these three cases we provide the optimal failure probability as well as the optimal measurement. We then apply our result to answer two relevant questions related to the implementation of the Bennett and Brassard 1984 cryptographic protocol. First 'With what probability can an eavesdropper unambiguously distinguish the *basis* of the signal?' and second 'With what probability can an eavesdropper unambiguously determine which *bit value* is sent without being interested in the knowledge of the basis?'.

This paper is organized as follows. In Section II we derive a theorem about the rank of the elements of an optimal USD measurement and give a corollary which takes the form of a reduction theorem. In Section III we present the exact solution for unambiguously discriminating two GU states in a four dimensional Hilbert space. In Section IV we consider two examples of practical interest in quantum cryptography. We then conclude in Section V.

II. RANK AND SPECTRUM OF THE ELEMENTS OF AN OPTIMAL USD MEASUREMENT

In Unambiguous State Discrimination the signal states must be identified without error. If those signal states are non-orthogonal quantum states, no perfect discrimination is possible and any USD measurement will lead to some inconclusive result. The rate of such inconclusive results is called the failure probability. Given a set of signal states ρ_i together with their *a priori* probabilities η_i we want to find an optimal measurement that minimizes the failure probability. The measurement is a generalized measurement, that is, a set of hermitian and positive semi-definite operators (or Positive Operator-Valued Measure [25]) $\{E_k\}_k$ that add up to the identity, i.e. $\sum_k E_k = \mathbb{1}$. Given a set of N signal states, we consider measurements with $N+1$ outcomes where N outcomes identify conclusively one and only one signal state while the last outcome indicates that the identification failed. The $N+1$ POVM elements are denoted by E_k, $k = 1, \ldots, N$, and $E_?$ respectively. The probability to obtain the outcome E for a state ρ is given by the trace quantity $\mathrm{Tr}(E\rho)$. Therefore the conditions for an error-free measurement simply is $\mathrm{Tr}(E_k\rho_i) = 0$ whenever $k \neq i$ so that only the state ρ_k can trigger the measurement outcome E_k. The failure probability Q to be optimized over all possible USD measurement is given by $Q = \sum_i \eta_i \mathrm{Tr}(E_?\rho_i)$. We often note Q_i the partial failure probability $\eta_i \mathrm{Tr}(E_?\rho_i)$.

In this paper we consider the unambiguous discrimination of two signal states ρ_0 and ρ_1 with *a priori* probabilities η_0 and η_1. Consequently our measurement contains three elements $\{E_0, E_1, E_?\}$ which correspond respectively to the conclusive detection of ρ_0, to the conclusive detection of ρ_1 and to an inconclusive result. For any hermitian and positive semi-definite operator A, we can introduce the notions of support, kernel and square root. The support $\mathcal{S}_A$ of A is the subspace spanned by the eigenvectors of A (eigenvectors associated with non zero eigenvalues). Its orthogonal complement is called the kernel of A and is denoted $\mathcal{K}_A$. The square root $\sqrt{A}$ of A is defined as the unique positive semi-definite operator such that $\sqrt{A}^2 = A$. This square root operator allows us to write decompositions of the form

$$A = MM^\dagger \text{ with } M = \sqrt{A}V, \tag{1}$$

for any unitary transformation V. Since the states ρ_i, $i = 0, 1$ and the POVM elements E_k, $k = 0, 1, ?$ are positive semi-definite operators, we can introduce their support, kernel, square root and decompositions of the form given in Eqn.(1).

We now derive upper bounds on the rank of the elements E_0 and E_1 of an optimal USD POVM. The object of our first theorem will be to see under which conditions these upper bounds can be reached. To start, we remember that the error-free condition $\mathrm{Tr}[E_i\rho_j] = 0$, $i, j = 0, 1$, $i \neq j$, implies the orthogonality between the support of E_i and the support of ρ_j [12]. Therefore $\mathcal{S}_{E_i} \subset \mathcal{K}_{\rho_j}$ and the dimension of the support $\mathcal{S}_{E_i}$, or equivalently the rank r_{E_i} of E_i, is upper bounded by the dimension of the kernel $\mathcal{K}_{\rho_j}$. We therefore end up with

$$\begin{aligned} r_{E_0} &\leq dim(\mathcal{K}_{\rho_1}), \\ r_{E_1} &\leq dim(\mathcal{K}_{\rho_0}). \end{aligned} \tag{2}$$

In the relevant case of two density matrices without overlapping supports, we will show that the rank of the USD

POVM elements E_i, $i = 0, 1$, simply is upper bounded by r_i, the rank of the mixed states ρ_i:

$$\begin{aligned} r_{E_0} &\leq r_0, \\ r_{E_1} &\leq r_1. \end{aligned} \tag{3}$$

Indeed if $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$, then $dim(\mathcal{H}) = dim(\mathcal{S}_{\rho_0}) + dim(\mathcal{S}_{\rho_1})$ and it follows that

$$\begin{aligned} r_{E_i} &\leq dim(\mathcal{K}_{\rho_j}), \;\; i = 0, 1, i \neq j \\ &= dim(\mathcal{H}) - dim(\mathcal{S}_{\rho_j}) \\ &\leq dim(\mathcal{S}_{\rho_0}) + dim(\mathcal{S}_{\rho_1}) - dim(\mathcal{S}_{\rho_j}) \\ &\leq dim(\mathcal{S}_{\rho_i}). \end{aligned} \tag{4}$$

Note for completeness that it has been already shown in [14] that the rank of $E_?$ is upper bounded by the smallest rank of the two density matrices ρ_0 and ρ_1:

$$r_{E_?} \leq min(r_0, r_1). \tag{5}$$

We are now ready to derive our first theorem. For this theorem, we assume two density matrices without overlapping supports, which can always be achieved using the reduction mechanism of [12]. The theorem states that the POVM elements E_0 and E_1 of an optimal USD measurement have rank r_0 and r_1, respectively, only if the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$ are positive semi-definite. The positivity of these two operators was already introduced in [14] as necessary and sufficient condition for the failure probability Q to reach the overall lower bound $2\sqrt{\eta_0\eta_1}F$, where F denotes the fidelity between the two density matrices. Here comes the precise statement.

Theorem 1 *Constraints on the rank of the two POVM elements E_0 and E_1 of an optimal USD measurement*
Consider a USD problem defined by two density matrices ρ_0 and ρ_1 and their respective a priori *probabilities η_0 and η_1 such that their supports satisfy $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ (Any USD problem of two density matrices can be reduced to such a form according to [12]). Consider also an optimal measurement $\{E_0^{opt}, E_1^{opt}, E_?^{opt}\}$ to that problem. Let F_0 and F_1 be the two operators $\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. The fidelity F of the two states ρ_0 and ρ_1 is then given by $F = Tr(F_0) = Tr(F_1)$. Let r_0 and r_1 be the rank of the two density matrices ρ_0 and ρ_1.*

If the POVM elements E_0^{opt} and E_1^{opt} have rank r_0 and r_1, respectively, then

$$\begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0 \geq 0, \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1 \geq 0. \end{cases} \tag{6}$$

The proof of this theorem relies on Eldar's necessary and sufficient conditions and on the tools and theorems derived in [14] (i.e. the notion of parallel addition, the theorem about the lower bound on the product Q_0Q_1, the theorem about the lower bound on the failure probability Q and the necessary and sufficient conditions to reach this lower bound). A detailled proof is given in Appendix A.

Theorem 1 suggests that the two POVM elements E_0 and E_1 have rank r_0 and r_1, respectively, only in a small regime of the ratio $\sqrt{\frac{\eta_1}{\eta_0}}$ around 1. This comes from the fact that the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1$ can be positive semi-definite only in a small regime of the ratio $\sqrt{\frac{\eta_1}{\eta_0}}$ around 1. Actually it has been already shown in [14] that the positivity of the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1$ is only possible when

$$\frac{\mathrm{Tr}(P_1\rho_0)}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{F}{\mathrm{Tr}(P_0\rho_1)}. \tag{7}$$

But the boundaries of this regime can even be made tighter. If more knowledge on the two density matrices ρ_0 and ρ_1 is provided, we can obtain tighter bounds. Such an example of tighter bounds is given in Appendix B.

A corollary of Theorem 1 can be stated if one assumes a standard form of USD problem. Indeed Theorem 1 can be rephrased as follows:

Whenever the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$ are not positive semi-definite, at least one of the two POVM elements E_i, $i = 0, 1$, of an optimal USD measurement does not have rank r_i.

In the case of two density matrices without overlapping supports, the rank of the USD POVM elements E_i, $i = 0, 1$, is upper bounded by r_i, the rank of the mixed states ρ_i. In the case of a standard form [33], the two density matrices ρ_0 and ρ_1 then have the same rank r in a $2r$-dimensional Hilbert space [14] and we end up with

$$\begin{aligned} r_{E_0} &\leq r, \\ r_{E_1} &\leq r, \\ r_{E_?} &\leq r. \end{aligned} \tag{8}$$

since $r_{E_?} \leq min(dim(\mathcal{S}_{\rho_0}), dim(\mathcal{S}_{\rho_1}))$ and $dim(\mathcal{S}_{\rho_0}) = dim(\mathcal{S}_{\rho_1}) = r$. A corollary to Theorem 1 can then be derived. If the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$ are not positive semi-definite, then a two-dimensional subspace can be split off from the original USD problem. This corollary actually is a fourth but incomplete reduction theorem. 'Reduction theorem' because no optimization is required onto that two-dimensional subspace. 'Incomplete' because the existence and the structure of this subspace are known but no complete analytical characterization is available yet. The precise statement of this Corollary follows.

Corollary 1 *A fourth, incomplete, reduction theorem*
Consider a standard USD problem defined by two density matrices ρ_0 and ρ_1 and their respective a priori probabilities η_0 and η_1 (any USD problem of two density matrices can be reduced to such a form according to [12]). Consider also

$$\textit{If the condition } \begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1 \geq 0 \end{cases} \textit{ is violated then} \tag{9}$$

there exists a two-dimensional subspace than can be split off from the original Hilbert space.

This two-dimensional subspace is characterized by a two-dimensional orthonormal basis $\{|e\rangle, |e'\rangle\}$ such that either

$$|e\rangle \in \mathcal{S}_{\rho_0} \textit{ and } |e'\rangle \in \mathcal{K}_{\rho_0} \textit{ and } \begin{cases} E_?^{opt}|e\rangle = |e\rangle \\ E_1^{opt}|e'\rangle = |e'\rangle \\ E_0^{opt}|e\rangle = E_0^{opt}|e'\rangle = E_1^{opt}|e\rangle = E_?^{opt}|e'\rangle = 0, \end{cases}$$

or

$$|e\rangle \in \mathcal{S}_{\rho_1} \textit{ and } |e'\rangle \in \mathcal{K}_{\rho_1} \textit{ and } \begin{cases} E_?^{opt}|e\rangle = |e\rangle \\ E_0^{opt}|e'\rangle = |e'\rangle \\ E_1^{opt}|e\rangle = E_1^{opt}|e'\rangle = E_0^{opt}|e\rangle = E_?^{opt}|e'\rangle = 0. \end{cases}$$

First let us note that this corollary makes the assumption of a *standard* USD problem. It is in principle not necessary to make such a strong assumption to derive the existence of some eigenvector of $E_?$, E_0 or E_1 with eigenvalue 1 since Theorem 1 is valid for any pair of density matrices without overlapping supports. Nevertheless Corollary 1 aims to be a fourth reduction theorem. It means in particular that, for any given USD problem of two density matrices, we would like to apply the 'four' reduction theorems and always end up with the optimal USD measurement.

The above corollary is a kind of incomplete *reduction theorem*. A reduction theorem is a theorem that allows us to decrease the size of a USD problem by splitting off some subspace onto which no optimization is needed. To have a complete reduction theorem here, we would need to characterize $|e\rangle$ and $|e'\rangle$ without solving the whole optimization problem. So far the existence of $|e\rangle$ and $|e'\rangle$ is ensured and their structure (they are eigenvectors of some POVM elements) is known. If $|e\rangle$ and $|e'\rangle$ were completely characterized in terms of ρ_0, ρ_1, η_0 and η_1, we would have a recipe to solve any USD problem. To see that let us assume that $|e\rangle$ and $|e'\rangle$ can be fully characterized and start with two generic mixed states.
In the following, the exponent (r) denotes the rank of the density matrices after reduction. First of all we use the first three reduction theorems to bring the problem into the standard form. We then check whether the two operators $\rho_0^{(r)} - \sqrt{\frac{\eta_1^{(r)}}{\eta_0^{(r)}}}F_0^{(r)}$ and $\rho_1^{(r)} - \sqrt{\frac{\eta_0^{(r)}}{\eta_1^{(r)}}}F_1^{(r)}$ are positive semi-definite. If yes then we know the optimal failure

probability as well as the optimal measurement to perform since this case falls into the first class of exact solutions [14]. If at least one of the two operators $\rho_0^{(r)} - \sqrt{\frac{\eta_1^{(r)}}{\eta_0^{(r)}}} F_0^{(r)}$ and $\rho_1^{(r)} - \sqrt{\frac{\eta_0^{(r)}}{\eta_1^{(r)}}} F_1^{(r)}$ is not positive semi-definite, we can use our last reduction theorem to get rid of a two-dimensional subspace and define the new density matrices $\rho_0^{(r-1)}$ and $\rho_1^{(r-1)}$ together with their respective *a priori* probabilities $\eta_0^{(r-1)}$ and $\eta_1^{(r-1)}$. At that point we check again the positivity of the two operators $\rho_0^{(r-1)} - \sqrt{\frac{\eta_1^{(r-1)}}{\eta_0^{(r-1)}}} F_0^{(r-1)}$ and $\rho_1^{(r-1)} - \sqrt{\frac{\eta_0^{(r-1)}}{\eta_1^{(r-1)}}} F_1^{(r-1)}$ of the reduced problem. We see here a constructive way to solve any USD problem. If the two operators $\rho_0^{(r')} - \sqrt{\frac{\eta_1^{(r')}}{\eta_0^{(r')}}} F_0^{(r')}$ and $\rho_1^{(r')} - \sqrt{\frac{\eta_0^{(r')}}{\eta_1^{(r')}}} F_1^{(r')}$, $r \geq r' \geq 2$, never happen to be positive, we end up with only two pure states and can finally find the optimal measurement (see Fig. 1). It remains that we cannot fully characterize $|e\rangle$ and $|e'\rangle$ even if we do know they exist and they are eigenvectors of some USD POVM elements. A detailled proof of Corollary 1 is given in Appendix C.

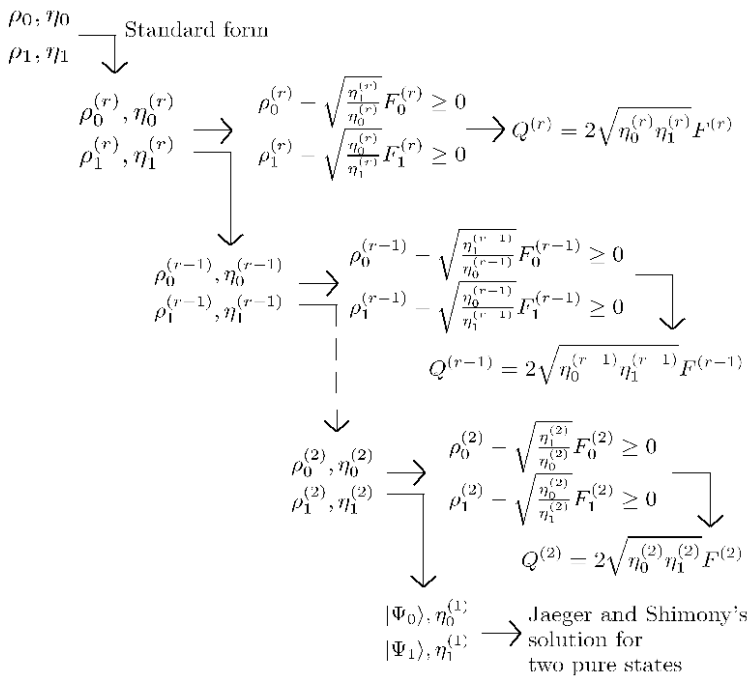

FIG. 1: A constructive way to solve any USD problem (the exponent $^{(r)}$ denotes the rank of the density matrices after reduction)

So far, there are only two ways to find a complete characterization of the two eigenvectors $|e\rangle$ and $|e'\rangle$ involved in Corollary 1. The first possibility is to consider a low dimensional USD problem. The second option is to consider a highly symmetric problem. The former case simply is the case of the two pure states where we want to unambiguously discriminate two pure states $|\Psi_0\rangle$ and $|\Psi_1\rangle$ with probabilities η_0 and η_1. Either the operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} \sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} \sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$ are positive semi-definite or we have $|e\rangle \in \mathcal{S}_{\rho_{0/1}}$, eigenvectors of $E_?$, and $|e'\rangle \in \mathcal{K}_{\rho_{0/1}}$, eigenvector of $E_{1/0}$. In only two dimensions, there is no freedom and $|e\rangle$ and $|e'\rangle$ must be $|\Psi_{0/1}\rangle$ and $|\Psi_{0/1}^{\perp}\rangle$. The two pure states case is solved extremely elegantly and extremely rapidly thanks to Corollary 1. If we are interested in higher dimensions we must consider a symmetry to give us enough constraints to fully characterize $|e\rangle$ and $|e'\rangle$. With the help of the Geometrically Uniform (GU) symmetry it is possible to go up to four dimensions and obtain the second class of exact solutions. This new class of solutions of generic USD problem is the object of the next section.

III. SECOND CLASS OF EXACT SOLUTIONS

Before deriving the next result of this paper, we need to introduce the so-called *Geometrically Uniform* (GU) states. GU states are a generalization of symmetric states [11, 23, 26, 27, 28, 29]. While symmetric state are

generated from one generator state and a single unitary transformation, GU states are generated from one generator and a group of unitaries. More precisely, a set of GU state is a set of density matrices $\{\rho_i\}$, $i = 0, ..., n-1$ such that $\rho_i = U_i \rho U_i^\dagger$ where ρ is an arbitrary density matrix called the *generator* and the set $\{U_i\}$, $i = 0, ..., n-1$ is a set of unitary matrices that form an Abelian group. In order not to break the symmetry of the states, we assume that the *a priori* probabilities are all equal to $\frac{1}{n}$. A consequence of the group structure of the set $\{U_i\}$ is that we can always consider U_0 as the identity and ρ_0 as the generator for a given set of GU states. We can therefore always write two GU states as ρ_0 and $\rho_1 = U\rho_0 U$ where U is an involution (i.e. a unitary transformation U such that $U^2 = \mathbb{1}$ and $U^\dagger = U$) with $\eta_0 = \eta_1 = \frac{1}{2}$. Let us note that two GU states are two symmetric states since only a single unitary is needed.

The GU states are interesting for both practical and theoretical considerations. On the practical side, real applications often exhibit strong symmetries like GU symmetry [34]. On the theoretical side, this symmetry allows us to seek for simpler conditions and aim for new results. We are now ready to present the main result of this paper, that is, the optimal failure probability for unambiguously discriminating two *geometrically uniform* states in a four dimensional Hilbert space and its corresponding optimal measurement [35].

Theorem 2 *Optimal unambiguous discrimination of two geometrically uniform states in four dimensions*
Consider a USD problem defined by two geometrically uniform states ρ_0 and ρ_1 of rank two with equal a priori probabilities and spanning a four-dimensional Hilbert space. Let F_0 and F_1 be the two operators $\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. The fidelity F of the two states ρ_0 and ρ_1 is then given by $F = Tr(F_0) = Tr(F_1)$. We denote by $P_0^\perp$ and $P_1^\perp$ the projectors onto the kernel of ρ_0 and ρ_1. The optimal failure probability Q^{opt} for USD then satisfies

$$
\begin{aligned}
&1.\ Q^{\text{opt}} = F \ \ \textit{if} \ \ \rho_0 - F_0 \geq 0 \\
&2.\ Q^{\text{opt}} = 1 - \langle x|\rho_0|x\rangle \ \ \textit{if} \ \ \begin{cases} \rho_0 - F_0 \ngeq 0 \\ Spect(P_1^\perp U P_1^\perp) = \{a, -b\}, \quad a, b \in \mathbb{R}^+ \end{cases} \\
&3.\ Q^{\text{opt}} = 1 \ \ \textit{otherwise},
\end{aligned}
\tag{10}
$$

where $P_1^\perp U P_1^\perp = a|0\rangle\langle 0| - b|1\rangle\langle 1|$ and $|x\rangle = \frac{1}{\sqrt{a+b}}(e^{iArg(\langle 0|\rho_0|1\rangle)}\sqrt{b}|0\rangle + \sqrt{a}|1\rangle)$.
The POVM elements that realize these optimal failure probabilities are given in the three respective cases by

$$
\begin{aligned}
&1.\ E_0 = \Sigma^{-1}\sqrt{\rho_0}\,(\rho_0 - F_0)\,\sqrt{\rho_0}\Sigma^{-1} \ \ \textit{where} \ \ \Sigma = \rho_0 + \rho_1 \\
&\quad E_1 = UE_0U \\
&\quad E_? = \mathbb{1} - E_0 - UE_0U \\
&2.\ E_0 = |x\rangle\langle x| \\
&\quad E_1 = UE_0U \\
&\quad E_? = \mathbb{1} - E_0 - UE_0U \\
&3.\ E_0 = 0 \\
&\quad E_1 = 0 \\
&\quad E_? = \mathbb{1}.
\end{aligned}
\tag{11}
$$

Proof We consider a USD problem defined by two *geometrically uniform* states ρ_0 and $\rho_1 = U\rho_0 U$, $U^2 = \mathbb{1}$, of rank two, spanning a four-dimensional Hilbert space. This means in particular that they do not have overlapping supports. Indeed $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ since $rank(\rho_0) + rank(\rho_1) = rank(\rho_0 + \rho_1)$ [13]. Since we already know that $r_{E_i} \leq r_i$, $i = 0, 1$ and $r_{E_?} \leq min(r_0, r_1)$, we simply have

$$
\begin{aligned}
r_{E_0} &\leq 2, \\
r_{E_1} &\leq 2, \\
r_{E_?} &\leq 2.
\end{aligned}
\tag{12}
$$

Note that this problem is in the standard form as soon as it has no block diagonal structure.

The symmetry between the two states ρ_0 and ρ_1 allows further simplifications. Actually Eldar proved in [23] that the optimal measurement to unambiguously discriminate *geometrically uniform* states can be chosen *geometrically uniform*, too. Thus the POVM elements are such that

$$\begin{aligned} E_0 \ &, \\ E_1 \ &= UE_0U, \\ E_? \ &= \mathbb{1} - E_0 - UE_0U \end{aligned} \tag{13}$$

In addition we know from the first class of exact solutions that (see Theorem 3 in Appendix A or [14]), for two density matrices ρ_0 and ρ_1 with equal *a priori* probabilities and without overlapping supports,

$$Q^{\text{opt}} = F \ \Leftrightarrow \ \begin{cases} \rho_0 - F_0 \geq 0 \\ \rho_1 - F_1 \geq 0. \end{cases} \tag{14}$$

This is even a stronger statement that the desired one since Theorem 3 gives us an equivalence where we only want an implication [36]. Due to the symmetry of the states $\rho_0 - F_0$ and $\rho_1 - F_1$ share the same spectrum and the above conditions reduce to

$$Q^{\text{opt}} = F \ \Leftrightarrow \quad \rho_0 - F_0 \geq 0. \tag{15}$$

If $\rho_0 - F_0 \ngeq 0$ then Theorem 1 tells us that at least one of the two POVM elements E_0 and E_1 does not have rank $r = 2$. Because of the symmetry $E_1 = UE_0U$, E_0 and E_1 have the same rank so that if $\rho_0 - F_0 \ngeq 0$ then $r_{E_0} = r_{E_1} < 2$. Equivalently if $\rho_0 - F_0 \ngeq 0$ then the two POVM elements E_0 and E_1 have either rank 1 or rank 0. If $r_{E_0} = r_{E_1} = 0$ then $E_? = \mathbb{1}$ and $Q = 1$. Let us now focus on the remaining case $r_{E_0} = r_{E_1} = 1$.

First we will prove that an optimal USD measurement such that $r_{E_0} = r_{E_1} = 1$ and $rank(E_?) \leq 2$ is necessary a projective measurement with $rank(E_?) = 2$. To do so we can introduce the unit vectors $|x\rangle \in \mathcal{K}_{\rho_1}$, $|y\rangle \in \mathcal{K}_{\rho_0}$ and the real numbers x and y in $]0; +\infty[$ (we could in principle restrict x and y to be in $]0; 1]$ because probabilities are smaller than 1) such that

$$E_0 = x|x\rangle\langle x| \geq 0, \tag{16}$$

$$E_1 = y|y\rangle\langle y| \geq 0. \tag{17}$$

We call $\mathcal{S}_{xy}$ the two dimensional subspace spanned by $|x\rangle$ and $|y\rangle$, P_{xy} the projection onto it and $P_{xy}^{\perp}$ the projector onto its orthogonal complement. From the definition of the subspace $\mathcal{S}_{xy}$ and the completeness relation $\sum_k E_k = \mathbb{1}$ we have

$$P_{xy}^{\perp} E_? P_{xy}^{\perp} = P_{xy}^{\perp}. \tag{18}$$

Therefore $rank(P_{xy}^{\perp} E_? P_{xy}^{\perp}) = rank(P_{xy}^{\perp}) = 2$ and $E_?$ must be at least of rank 2. However we already know that $rank(E_?) \leq 2$ due to Eqn.(12). Therefore $rank(E_?) = 2$ and

$$E_? = P_{xy}^{\perp}. \tag{19}$$

We can now consider the subspace $\mathcal{S}_{xy}$ only. On that subspace, we have

$$E_0 + E_1 = P_{xy} \tag{20}$$

that is to say $P_{xy} = x|x\rangle\langle x| + y|y\rangle\langle y|$. Since P_{xy} is a projector, $P_{xy} = P_{xy}^2$ and it follows that $x^2|x\rangle\langle x| + y^2|y\rangle\langle y| + xy\langle y|x\rangle|y\rangle\langle x| + xy\langle y|x\rangle|y\rangle\langle x| = x|x\rangle\langle x| + y|y\rangle\langle y|$. The off-diagonal terms are equal if and only if $\langle y|x\rangle = 0$ ($x \neq 0$ and $y \neq 0$) while the diagonal terms are equal if and only if $x = y = 1$. The POVM then is a projective measurement with $rank(E_?) = 2$, $r_{E_0} = r_{E_1} = 1$.

We now give the optimal USD measurement for a GU projective measurement. Since the measurement is made of projectors, we have $\text{Tr}(E_0E_1) = 0$ or simply $\langle x|U|x\rangle = 0$. Since $|x\rangle$ lies in $\mathcal{K}_{\rho_1}$, this last relation is equivalent to

$$\langle x|P_1^{\perp} U P_1^{\perp}|x\rangle = 0. \tag{21}$$

$P_1^\perp U P_1^\perp$ is a hermitian operator, it therefore has real eigenvalues. Since $P_1^\perp$ is of rank 2, $P_1^\perp U P_1^\perp$ is at most of rank 2 too. We denote a and c the two eigenvalues of $P_1^\perp U P_1^\perp$ and $|0\rangle$ and $|1\rangle$ its two corresponding eigenvectors. In this eigenbasis $\{|0\rangle, |1\rangle\}$, $|x\rangle \in \mathcal{K}_{\rho_1}$ can be expressed as

$$|x\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \tag{22}$$

This yields $\langle x|P_1^\perp U P_1^\perp|x\rangle = |\alpha|^2 a + |\beta|^2 c$. Importantly this expression can only vanish if either $a > 0$ and $c < 0$ or $a = c = 0$. But in the later case, $P_1^\perp U P_1^\perp = 0$ implies that $P_1^\perp P_0^\perp = 0$. The two mixed states then are orthogonal and the operator $F_0 = 0$ so that $\rho_0 - F_0 = \rho_0 \geq 0$. This contradicts our assumption $\rho_0 - F_0 \ngeq 0$. Therefore we have $a > 0$ and $c < 0$ and we shall call $-c = b > 0$ such that, in the eigenbasis $\{|0\rangle, |1\rangle\}$,

$$P_1^\perp U P_1^\perp = \begin{pmatrix} a & 0 \\ 0 & -b \end{pmatrix}. \tag{23}$$

If we also consider the normalization of $|x\rangle$, we end up with a system of two equations. This system simply is

$$\begin{cases} |\alpha|^2 a - |\beta|^2 b = 0 \\ |\alpha|^2 + |\beta|^2 = 1 \end{cases}. \tag{24}$$

Up to a global phase, it admits a family of solutions parametrized by a relative phase $\Phi \in [0; 2\pi[$:

$$\{\alpha = \frac{e^{i\Phi}}{\sqrt{1 + a/b}}, \beta = \frac{1}{\sqrt{1 + b/a}}\}. \tag{25}$$

In the eigenbasis $\{|0\rangle, |1\rangle\}$ we can therefore write

$$|x\rangle = \begin{pmatrix} \frac{e^{i\Phi}}{\sqrt{1+a/b}} \\ \frac{1}{\sqrt{1+b/a}} \end{pmatrix}. \tag{26}$$

We then use again the fact that we are interested in the optimal measurement. Note that we already invoked the scenario of optimality when we stated state that for $\rho_0 - F_0 \ngeq 0$, the POVM is either $\{E_0 = E_1 = 0, E_? = \mathbb{1}\}$ or a projective measurement. Indeed Theorem 1 is only concerned with optimal USD POVMs. So far $|x\rangle$ is valid for any USD projective measurement that is GU symmetric. Let us now find the optimal one. To do so, we evaluate the success probability $P_{success}$ corresponding to our projective measurement. Because of the symmetry of the two GU states, $\mathrm{Tr}(E_0\rho_0) = \mathrm{Tr}(E_1\rho_1)$ and the success probability $P_{success} = \frac{1}{2}\mathrm{Tr}(E_0\rho_0) + \frac{1}{2}\mathrm{Tr}(E_1\rho_1)$ for unambiguously discriminating the two GU state ρ_0 and ρ_1 takes the form

$$P_{success} = \mathrm{Tr}(E_0\rho_0) = \langle x|\rho_0|x\rangle. \tag{27}$$

After calculation, we obtain

$$P_{success} = \frac{1}{a+b}\left(b\langle 0|\rho_0|0\rangle + a\langle 1|\rho_0|1\rangle + 2\sqrt{ab}Re(\langle 0|\rho_0|1\rangle e^{-i\Phi})\right). \tag{28}$$

To maximize the success probability $P_{success}$, we choose Φ such that $Re(\langle 0|\rho_0|1\rangle e^{-i\Phi}) = |\langle 0|\rho_0|1\rangle|$. Φ must therefore be equal to $Arg(\langle 0|\rho_0|1\rangle)$ and

$$|x\rangle = \begin{pmatrix} \frac{e^{iArg(\langle 0|\rho_0|1\rangle)}}{\sqrt{1+a/b}} \\ \frac{1}{\sqrt{1+b/a}} \end{pmatrix}. \tag{29}$$

This completes the proof. ■

Actually this last result shows that as soon as $\rho_0 - F_0 \ngeq 0$ the optimal measurement is 2x2 block diagonal even if the two states ρ_0 and ρ_1 are not! Moreover, it should be emphasised that Theorem 1 and Corollary 1 together provide a new insight into USD. The pure state case and the second class of exact solutions happen to be simple consequences of these theorems. Moreover Theorem 1 and Corollary 1 as well as the two classes of exact solutions known so far involve the operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. Our approach is in contrast to

recent works [22, 24, 30] where the emphasis is on the so-called canonical vectors rather than on the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$.

In the next section we consider an example of both theoretical and practical interest. In fact, we consider the *Bennett and Brassard 1984* protocol (BB84 protocol) implemented through weak coherent pulses with a strong phase reference.

IV. APPLICATION OF THE SECOND CLASS OF EXACT SOLUTIONS TO THE BB84 PROTOCOL

The Bennett and Brassard 1984 cryptographic protocol [31] provides a method to distribute a private key between two parties and therefore allow an unconditionally secure communication. We consider in this section the implementation of a BB84-type Quantum Key Distribution (QKD) protocol that uses weak coherent pulses with a phase reference [32]. In that context, two important questions related to unambiguous state discrimination can be addressed. First, 'With what probability can an eavesdropper unambiguously distinguish the *basis* of the signal?' and second 'With what probability can an eavesdropper unambiguously determine which *bit value* is sent without being interested in the knowledge of the basis?' These two questions can be translated in some unambiguous discrimination task concerning two *geometrically uniform* mixed states in a four dimensional Hilbert space. We answer these two questions providing useful insights for further investigations on practical implementations of Quantum Key Distribution protocols. Note that the details of all the following calculations can be found in [13].

A. The four signal states

The implementation of the BB84 considered here makes use of the four quantum optical coherent states $\{|\pm\alpha\rangle, |\pm i\alpha\rangle\}$[37]. Note that a coherent state $|\alpha\rangle$ is characterized by its complex amplitude $\alpha \in \mathbb{C}$ and is given in terms of the number states $|n\rangle$ as

$$|\alpha\rangle = e^{\frac{-|\alpha|^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}|n\rangle. \tag{30}$$

In that implementation the *bit value* is encoded in the sign of the coherent states. In other words, $|\alpha\rangle$ and $|i\alpha\rangle$ correspond to the *bit value* 0 while $|-\alpha\rangle$ and $|-i\alpha\rangle$ correspond to the *bit value* 1. Moreover the phase i plays the role of the basis in the standard BB84 protocol. Furthermore it is worth noticing that the states corresponding to the *bit value* 0 and 1 are not orthogonal since

$$\langle\alpha|-\alpha\rangle \neq 0, \tag{31}$$
$$\langle i\alpha|-i\alpha\rangle \neq 0. \tag{32}$$

In fact the first question refers to the unambiguous discrimination of the two *basis* $\{|\pm\alpha\rangle\}$ and $\{|\pm i\alpha\rangle\}$. We can build a mixed state ρ_r that corresponds to the basis $\{|\pm\alpha\rangle\}$ and a mixed state ρ_i for the basis $\{|\pm i\alpha\rangle\}$. The index 'i', for 'imaginary', refers to the imaginary number i multiplying the complex amplitude $\pm\alpha$ in the two states $\{|\pm i\alpha\rangle\}$ while the index 'r', for 'real', refers to the absence of this imaginary number i in $\{|\pm\alpha\rangle\}$. We end up with

$$\rho_r = \frac{1}{2}\left(|\alpha\rangle\langle\alpha| + |-\alpha\rangle\langle-\alpha|\right), \tag{33}$$
$$\rho_i = \frac{1}{2}\left(|i\alpha\rangle\langle i\alpha| + |-i\alpha\rangle\langle-i\alpha|\right). \tag{34}$$

The second question refers to the unambiguous discrimination of the two *bit value* mixed states. For that case we can build the two density matrices

$$\rho_0 = \frac{1}{2}\left(|\alpha\rangle\langle\alpha| + |i\alpha\rangle\langle i\alpha|\right), \tag{35}$$
$$\rho_1 = \frac{1}{2}\left(|-\alpha\rangle\langle-\alpha| + |-i\alpha\rangle\langle-i\alpha|\right). \tag{36}$$

Here the indexes 0 and 1 refer to the bit value.
It now remains to write these four density matrices in a four dimensional Hilbert space. Actually the states $\{|\pm\alpha\rangle, |\pm i\alpha\rangle\}$ are four linearly independent pure states. Therefore they span a four dimension Hilbert space.

We denote these four signal states as

$$|\Psi_0\rangle = |\alpha\rangle, \tag{37}$$
$$|\Psi_1\rangle = |i\alpha\rangle, \tag{38}$$
$$|\Psi_2\rangle = |-\alpha\rangle, \tag{39}$$
$$|\Psi_3\rangle = |-i\alpha\rangle. \tag{40}$$

In the phase space, these four states are generated from $|\Psi_0\rangle = |\alpha\rangle$ and a rotation of angle $\frac{\pi}{2}$. This means they are symmetric states and can be written in a suitable basis following Chefles *et al.* [6]. The idea is that n symmetric states $|\Psi_k\rangle$ can always be written in an orthonormal basis $\{|\Phi_j\rangle\}$ as

$$|\Psi_k\rangle = \sum_{j=0}^{n-1} c_j e^{2i\pi\frac{kj}{n}} |\Phi_j\rangle. \tag{41}$$

Note that the phase of the complex numbers c_j is not relevant since we can absorb it in the definition of the basis elements $|\Phi_j\rangle$. Finally the modulus of the coefficients c_j's can be expressed [6] as

$$|c_j|^2 = \frac{1}{n^2} \sum_{k,k'} e^{-2i\pi\frac{j(k-k')}{n}} \langle\Psi_{k'}|\Psi_k\rangle. \tag{42}$$

In the orthonormal basis $\{|\Phi_j\rangle\}$, our four symmetric states are finally expressed as

$$|\Psi_0\rangle = \begin{pmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{pmatrix}, |\Psi_1\rangle = \begin{pmatrix} c_0 \\ ic_1 \\ -c_2 \\ -ic_3 \end{pmatrix}, |\Psi_2\rangle = \begin{pmatrix} c_0 \\ -c_1 \\ c_2 \\ -c_3 \end{pmatrix}, |\Psi_3\rangle = \begin{pmatrix} c_0 \\ -ic_1 \\ -c_2 \\ ic_3 \end{pmatrix}, \tag{43}$$

and we obtain the coefficients c_i's as functions of the mean photon number $\mu = |\alpha|^2$ of the coherent pulse:

$$c_0 = \frac{1}{\sqrt{2}} e^{-\frac{\mu}{2}} \sqrt{\cosh(\mu) + \cos(\mu)}, \tag{44}$$
$$c_1 = \frac{1}{\sqrt{2}} e^{-\frac{\mu}{2}} \sqrt{\sinh(\mu) + \sin(\mu)}, \tag{45}$$
$$c_2 = \frac{1}{\sqrt{2}} e^{-\frac{\mu}{2}} \sqrt{\cosh(\mu) - \cos(\mu)}, \tag{46}$$
$$c_3 = \frac{1}{\sqrt{2}} e^{-\frac{\mu}{2}} \sqrt{\sinh(\mu) - \sin(\mu)}. \tag{47}$$

B. USD of the *basis* mixed states

The first question refers to the USD of the following two density matrices:

$$\rho_r = \begin{pmatrix} c_0^2 & 0 & c_0c_2 & 0 \\ 0 & c_1^2 & 0 & c_1c_3 \\ c_0c_2 & 0 & c_2^2 & 0 \\ 0 & c_1c_3 & 0 & c_3^2 \end{pmatrix} \tag{48}$$

and

$$\rho_i = \begin{pmatrix} c_0^2 & 0 & -c_0c_2 & 0 \\ 0 & c_1^2 & 0 & -c_1c_3 \\ -c_0c_2 & 0 & c_2^2 & 0 \\ 0 & -c_1c_3 & 0 & c_3^2 \end{pmatrix}. \tag{49}$$

One can actually calculate the spectrum of the operator $\rho_r - F_r$ and find that

$$Spect(\rho_r - F_r) = \{max\{c_0^2, c_2^2\}, max\{c_1^2, c_3^2\}\}\} \tag{50}$$

which is positive for any value of μ. Therefore Theorem 2 tells us that $Q^{opt} = F$ for any value of μ. One can also calculate the fidelity which takes the form $F = |c_0^2 - c_2^2| + |c_1^2 - c_3^2|$. In terms of the mean photon number the optimal failure probability (see Fig. 2) is finally expressed as

$$Q^{opt} = e^{-\mu} \left(|\cos \mu| + |\sin \mu| \right), \forall \mu. \tag{51}$$

The corresponding optimal measurement is, moreover, given by

$$\begin{aligned} E_r &= \Sigma^{-1} \sqrt{\rho_r} \left(\rho_r - F_r \right) \sqrt{\rho_r} \Sigma^{-1} \\ E_i &= U E_r U \\ E_? &= \mathbb{1} - E_r - U E_r U \end{aligned} \tag{52}$$

where Σ^{-1} simply is

$$\begin{pmatrix} c_0^{-2} & 0 & 0 & 0 \\ 0 & c_1^{-2} & 0 & 0 \\ 0 & 0 & c_2^{-2} & 0 \\ 0 & 0 & 0 & c_3^{-2} \end{pmatrix}. \tag{53}$$

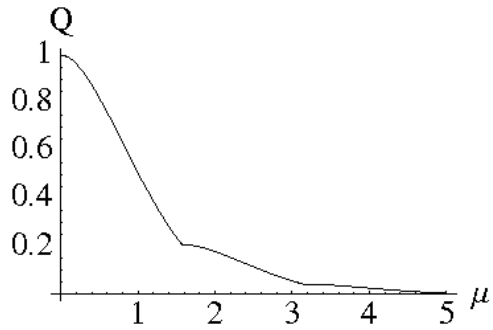

FIG. 2: Optimal failure probability for USD of the *basis* mixed states

C. USD of the *bit value* mixed states

The second question refers to the USD of the following two density matrices:

$$\rho_0 = \begin{pmatrix} c_0^2 & \frac{1-i}{2} c_0 c_1 & 0 & \frac{1+i}{2} c_0 c_3 \\ \frac{1+i}{2} c_1 c_0 & c_1^2 & \frac{1-i}{2} c_1 c_2 & 0 \\ 0 & \frac{1+i}{2} c_2 c_1 & c_2^2 & \frac{1-i}{2} c_2 c_3 \\ \frac{1-i}{2} c_3 c_0 & 0 & \frac{1+i}{2} c_3 c_2 & c_3^2 \end{pmatrix} \tag{54}$$

and

$$\rho_1 = \begin{pmatrix} c_0^2 & -\frac{1-i}{2} c_0 c_1 & 0 & -\frac{1+i}{2} c_0 c_3 \\ -\frac{1+i}{2} c_1 c_0 & c_1^2 & -\frac{1-i}{2} c_1 c_2 & 0 \\ 0 & -\frac{1+i}{2} c_2 c_1 & c_2^2 & -\frac{1-i}{2} c_2 c_3 \\ -\frac{1-i}{2} c_3 c_0 & 0 & -\frac{1+i}{2} c_3 c_2 & c_3^2 \end{pmatrix}. \tag{55}$$

The spectrum of the operator $\rho_0 - F_0$ is now given by

$$Spect(\rho_0 - F_0) = \frac{1}{2} \left(1 - e^{-\mu} \pm e^{-2\mu} \sqrt{1 + e^{2\mu} - 2e^{\mu} \cos(2\mu)} \right). \tag{56}$$

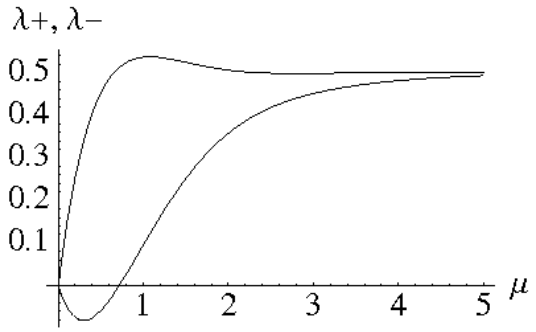

FIG. 3: Spectrum of the operator $\rho_0 - F_0$ for USD of the *bit value* mixed states

This spectrum is not always positive (see Fig. 3). Indeed only in a regime of relatively large μ ($\mu \geq \mu_0 \approx 0.7193$ photon per pulse), the quantity $\frac{1}{2}(1 - e^{-\mu} - e^{-2\mu}\sqrt{1 + e^{2\mu} - 2e^{\mu}\cos(2\mu)}$ is greater than 0. In the regime $\mu \geq \mu_0$, the positivity of the operator $\rho_0 - F_0$ ensures that the optimal failure probability reaches the fidelity bound F, which can be expresses as $e^{-\mu}$ (See [13] for details). We therefore obtain (see Fig. 4)

$$Q^{\text{opt}} = e^{-\mu}, \forall \mu \geq \mu_0. \tag{57}$$

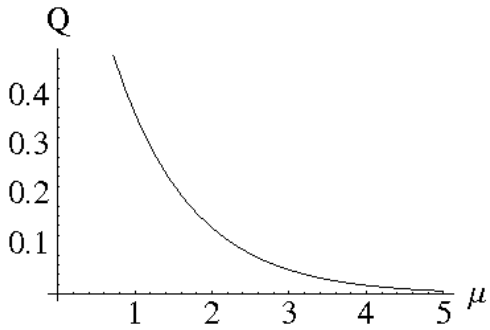

FIG. 4: Optimal failure probability for USD of the *bit value* mixed states for $\mu \geq \mu_0$

The corresponding optimal measurement is moreover given by

$$\begin{aligned} E_0 &= \Sigma^{-1}\sqrt{\rho_0}\,(\rho_0 - F_0)\,\sqrt{\rho_0}\Sigma^{-1} \\ E_1 &= UE_0U \\ E_? &= \mathbb{1} - E_0 - UE_0U \end{aligned} \tag{58}$$

where Σ^{-1} still equals

$$\begin{pmatrix} c_0^{-2} & 0 & 0 & 0 \\ 0 & c_1^{-2} & 0 & 0 \\ 0 & 0 & c_2^{-2} & 0 \\ 0 & 0 & 0 & c_3^{-2} \end{pmatrix}. \tag{59}$$

Note that for $\mu = \mu_0$, the POVM elements E_0 and E_1 have rank 1 since one eigenvalue of $\rho_0 - F_0$ vanishes.

In the regime $\mu < \mu_0$ where the operator $\rho_0 - F_0$ is not positive semi-definite we must look at the spectrum of the operator $P_1^{\perp}UP_1^{\perp}$. This spectrum does not give a convenient analytic form since we leave the protocol parameter μ open. We, therefore, evaluate it numerically. It turns out that the spectrum always has two eigenvalues of opposite sign in the regime $\mu < \mu_0$. Consequently we can write the operator $P_1^{\perp}UP_1^{\perp}$ in its eigenbasis $\{|0\rangle, |1\rangle\}$ as

$$P_1^{\perp}UP_1^{\perp} = a|0\rangle\langle 0| - b|1\rangle\langle 1|, \;\; a, b \in \mathbb{R}^+. \tag{60}$$

And in virtue of Theorem 1, the optimal failure probability for unambiguously discriminating the *bit value* mixed states is given by

$$Q^{\text{opt}} = 1 - \frac{1}{a+b}(b\langle 0|\rho_0|0\rangle + a\langle 1|\rho_0|1\rangle + 2\sqrt{ab}|\langle 0|\rho_0|1\rangle|), \forall \mu < \mu_0. \tag{61}$$

The complete graph for the failure probability is shown on Fig. 5

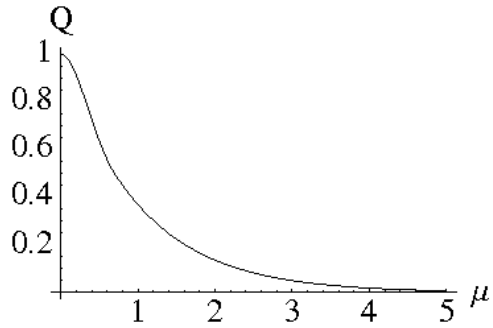

FIG. 5: Optimal failure probability for USD of the *bit value* mixed states

So far no neat expression for the optimal failure probability is known in terms of μ for $\mu < \mu_0$. This comes from the rather complicated form of the states ρ_0 and ρ_1 and the fact that no analytical expression of P_0 and P_1 is known. Let us finally add that the optimal USD measurement is, in the eigenbasis of $P_1^{\perp} U P_1^{\perp}$, of form

$$\begin{array}{l} E_0 = |x\rangle\langle x| \\ E_1 = U E_0 U \\ E_? = \mathbb{1} - E_0 - U E_0 U \end{array} \quad with\ |x\rangle = \begin{pmatrix} \frac{e^{iArg(\langle 0|\rho_0|1\rangle)}}{\sqrt{1+a/b}} \\ \frac{1}{\sqrt{1+b/a}} \\ 0 \\ 0 \end{pmatrix}. \tag{62}$$

Here again we cannot write these operators in terms of the mean photon number μ. On Fig.6 we finally compare the optimal failure probabilities for USD of the *basis* and the *bit value* mixed states.

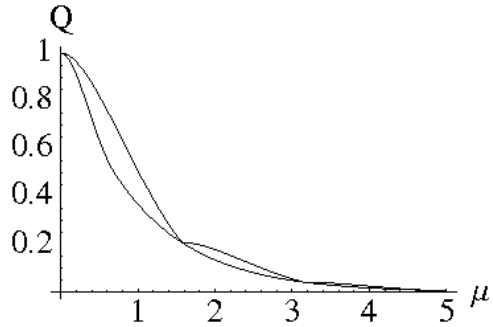

FIG. 6: Comparison between the optimal failure probabilities for USD of the *basis* and the *bit value* mixed states

V. CONCLUSION

In this paper we have provided a partial fourth reduction theorem. This theorem tells us that either the failure probability equals the overall lower bound $2\sqrt{\eta_0\eta_1}F$ or a two dimensional subspace can split off from the original Hilbert space. In fact, this result can be used as a toolbox to go beyond special cases and solve analytically USD problems that can not be solved with the help of the three reduction theorems. We have then employed this partial reduction theorem to derive a second class of exact solutions. This class corresponds to any pair of geometrically uniform states in a four dimensional Hilbert space. For that class of states we give the optimal failure probability

as well as the associated optimal measurement. As an application, we have used this result to address two questions related to the implementation of the BB84 QKD protocol with weak coherent states. The questions 'With what probability can an eavesdropper unambiguously distinguish the *basis* of the signal?' and 'With what probability can an eavesdropper unambiguously determine which *bit value* is sent without being interested in the knowledge of the basis?' are each related to the unambiguous discrimination of a pair of geometrically uniform states in a four dimensional Hilbert space.

Acknowledgments

We would like to thank Matthias Kleinmann, Hermann Kampermann and Dagmar Bruss for useful discussions. This work was supported by the DFG under the Emmy-Noether program and the EU Integrated Project QAP.

VI. APPENDICES

Appendix A: Proof of Theorem 1

We now proof Theorem 1 which is repeated here:

Theorem 1 Constraints on the rank of the two POVM elements E_0 and E_1 of an optimal USD measurement *Consider a USD problem defined by two density matrices ρ_0 and ρ_1 and their respective* a priori *probabilities η_0 and η_1 such that their supports satisfy $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ (Any USD problem of two density matrices can be reduced to such a form according to [12]). Consider also an optimal measurement $\{E_0^{opt}, E_1^{opt}, E_?^{opt}\}$ to that problem. Let F_0 and F_1 be the two operators $\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. The fidelity F of the two states ρ_0 and ρ_1 is then given by $F = Tr(F_0) = Tr(F_1)$. Let r_0 and r_1 be the rank of the two density matrices ρ_0 and ρ_1.*

If the POVM elements E_0^{opt} and E_1^{opt} have rank r_0 and r_1, respectively, then

$$\begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0 \geq 0, \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1 \geq 0. \end{cases} \tag{63}$$

This theorem is concerned with an optimal measurement for unambiguously discriminating two mixed states ρ_0 and ρ_1. We can therefore use the necessary and sufficient conditions derived by Eldar in [23]. We recall them here in a language adapted to our calculations.

A necessary and sufficient condition for a measurement $\{E_k\}$, $k \in \{0, 1, ?\}$, to be optimal is the existence of a positive semi-definite operator Z such that

$$ZE_? = 0, \tag{64}$$
$$E_0(Z - \eta_0\rho_0)E_0 = 0, \tag{65}$$
$$E_1(Z - \eta_1\rho_1)E_1 = 0, \tag{66}$$
$$P_1^{\perp}(Z - \eta_0\rho_0)P_1^{\perp} \geq 0, \tag{67}$$
$$P_0^{\perp}(Z - \eta_1\rho_1)P_0^{\perp} \geq 0, \tag{68}$$

where $P_i^{\perp}$ is the projector onto the kernel of ρ_i, $i = 0, 1$.

The proof of Theorem 1 can be decomposed in five steps. The first step corresponds to the restriction of Eldar's necessary and sufficient conditions to the case where the POVM elements E_0 and E_1 of a USD measurement have rank r_0 and r_1, respectively. After some calculations, this will provide us a first statement:

If the two POVM elements E_0 and E_1 of an optimal USD measurement have rank r_0 and r_1, respectively, then

$$\exists Z \geq 0 \text{ such that } \begin{cases} ZE_? = 0 \\ P_0^{\perp}(Z - \eta_1\rho_1)P_0^{\perp} = 0 \\ P_1^{\perp}(Z - \eta_0\rho_0)P_1^{\perp} = 0 \end{cases}. \tag{69}$$

Therefore, to prove Theorem 1, we will simply have to show the equivalence:

$$\exists Z \geq 0 \text{ such that } \begin{cases} ZE_? = 0 \\ P_0^{\perp}(Z - \eta_1\rho_1)P_0^{\perp} = 0 \\ P_1^{\perp}(Z - \eta_0\rho_0)P_1^{\perp} = 0 \end{cases} \Leftrightarrow \begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}} F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}} F_1 \geq 0 \end{cases}. \tag{70}$$

The remaining four steps will show this equivalence. More precisely, the second step makes use of the notion of parallel addition. The third step uses the positive semi-definiteness of the unknown operator Z and focus on the equation $ZE_? = 0$. The fourth step is concerned with the optimal failure probability. The fifth and final step uses an equivalence already shown in [14].

First step
In that first step, we only want to prove an implication. First of all let us repeat that $dim(\mathcal{K}_{\rho_i}) = r_j$, $i, j \in \{0, 1\}$,

$i \neq j$ since the supports of ρ_0 and ρ_1 do not overlap. We will now see the following:

If the USD POVM is optimal, i.e. Eqn.(64) to (68) are fulfilled, and E_0 and E_1 have rank r_0 and r_1, respectively, then the two hermitian operators $P_1^\perp(Z-\eta_0\rho_0)P_1^\perp$ and $P_0^\perp(Z-\eta_1\rho_1)P_0^\perp$ must vanish.

Indeed the situation is the following: We consider two positive semi-definite operators A and B, with A having full rank and $ABA^\dagger = 0$. We can see this relation as of the form $CC^\dagger = 0$ with $C = A\sqrt{B}$. Such an equation $CC^\dagger = 0$ is equivalent to $C = 0$ for any matrix C. Consequently, $ABA^\dagger = 0$ is equivalent to $A\sqrt{B} = 0$. Finally, since A is full rank, A^{-1} exists and B must vanish.

Let us now focus on Eqn.(65) where E_0 and $P_1^\perp(Z-\eta_0\rho_0)P_1^\perp$ both have support in $\mathcal{K}_{\rho_1}$. We assume $r_{E_0} = dim(\mathcal{K}_{\rho_1}) = r_0$ so that on the subspace $\mathcal{K}_{\rho_1}$ we can consider E_1 as being full rank. We then set $A = E_0$ and $B = P_1^\perp(Z-\eta_0\rho_0)P_1^\perp$. Eqn.(65) tells us that $ABA^\dagger = 0$ with A full rank on $\mathcal{K}_{\rho_1}$ thus $B = P_1^\perp(Z-\eta_0\rho_0)P_1^\perp$ must vanish.
We can follow the same idea for Eqn.(66). We set $A = E_1$ and $B = P_0^\perp(Z-\eta_1\rho_1)P_0^\perp$. Since we assume $r_{E_1} = dim(\mathcal{K}_{\rho_0}) = r_1$, E_1 can be considered as being full rank in $\mathcal{K}_{\rho_0}$ and therefore $P_0^\perp(Z-\eta_1\rho_1)P_0^\perp$ must vanish. Therefore we obtain that:

If the two POVM elements E_0 and E_1 of an optimal USD measurement have rank r_0 and r_1, respectively, then

$$\exists Z \geq 0 \text{ such that } \begin{cases} ZE_? = 0 \\ P_0^\perp(Z-\eta_1\rho_1)P_0^\perp = 0 \\ P_1^\perp(Z-\eta_0\rho_0)P_1^\perp = 0 \\ P_0^\perp(Z-\eta_1\rho_1)P_0^\perp \geq 0 \\ P_1^\perp(Z-\eta_0\rho_0)P_1^\perp \geq 0 \end{cases} . \tag{71}$$

The above statement finally implies that:

If the two POVM elements E_0 and E_1 of an optimal USD measurement have rank r_0 and r_1, respectively, then

$$\exists Z \geq 0 \text{ such that } \begin{cases} ZE_? = 0 \\ P_0^\perp(Z-\eta_1\rho_1)P_0^\perp = 0 \\ P_1^\perp(Z-\eta_0\rho_0)P_1^\perp = 0 \end{cases} . \tag{72}$$

It now remains to show the following equivalence to prove Theorem 1:

$$\exists Z \geq 0 \text{ such that } \begin{cases} ZE_? = 0 \\ P_0^\perp(Z-\eta_1\rho_1)P_0^\perp = 0 \\ P_1^\perp(Z-\eta_0\rho_0)P_1^\perp = 0 \end{cases} \Leftrightarrow \begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1 \geq 0 \end{cases} . \tag{73}$$

Second step
Since the supports of the two density matrices ρ_0 and ρ_1 do not overlap, we can make use of the notion of parallel addition and introduce the full rank operator $\Sigma^{-1} = (\rho_0+\rho_1)^{-1}$ [14]. Its main property lies in the relation:

$$\rho_i\Sigma^{-1}\rho_j = \rho_i\delta_{ij}, \;\; i = 0, 1. \tag{74}$$

As a consequence we get the interesting equalities

$$\rho_0\Sigma^{-1} = \rho_0\Sigma^{-1}P_1^\perp, \tag{75}$$

$$P_1^\perp\rho_0\Sigma^{-1} = P_1^\perp. \tag{76}$$

Indeed $\rho_0\Sigma^{-1} = \rho_0\Sigma^{-1}(P_1+P_1^\perp) = \rho_0\Sigma^{-1}\rho_1\rho_1^{-1} + \rho_0\Sigma^{-1}P_1^\perp = \rho_0\Sigma^{-1}P_1^\perp$. Moreover, $P_1^\perp = P_1^\perp\mathbb{1} = P_1^\perp(\rho_0+\rho_1)\Sigma^{-1} = P_1^\perp\rho_0\Sigma^{-1}$.

If we now consider the equation $P_1^\perp(Z-\eta_0\rho_0)P_1^\perp = 0$. We can multiply it on the left by $\rho_0\Sigma^{-1}$ and on the right by $\Sigma^{-1}\rho_0$. We then have

$$\rho_0\Sigma^{-1}P_1^\perp(Z-\eta_0\rho_0)P_1^\perp\Sigma^{-1}\rho_0 = 0. \tag{77}$$

Because of Eqn. (75), this implies

$$\rho_0\Sigma^{-1}(Z-\eta_0\rho_0)\Sigma^{-1}\rho_0 = 0. \tag{78}$$

We can also go in the other direction. Indeed it follows from the previous equation that:

$$P_1^{\perp}\rho_0\Sigma^{-1}(Z-\eta_0\rho_0)\Sigma^{-1}\rho_0 P_1^{\perp}=0 \tag{79}$$

which together with Eqn. (76) yield

$$P_1^{\perp}(Z-\eta_0\rho_0)P_1^{\perp}=0. \tag{80}$$

Consequently $P_1^{\perp}(Z-\eta_0\rho_0)P_1^{\perp}=0$ and $\rho_0\Sigma^{-1}(Z-\eta_0\rho_0)\Sigma^{-1}\rho_0=0$ are equivalent propositions for two density matrices without overlapping supports. The same result is of course true when we swap 0 and 1. Therefore, $P_0^{\perp}(Z-\eta_1\rho_1)P_0^{\perp}=0$ and $\rho_1\Sigma^{-1}(Z-\eta_1\rho_1)\Sigma^{-1}\rho_1=0$ are equivalent too.

We now come back to the equivalence (73). Thanks to the previous discussion, the proposition

$$\exists Z\geq 0 \text{ such that } \begin{cases} ZE_? = 0 \\ P_0^{\perp}(Z-\eta_1\rho_1)P_0^{\perp}=0 \\ P_1^{\perp}(Z-\eta_0\rho_0)P_1^{\perp}=0 \end{cases} \tag{81}$$

can be advantageously replaced by

$$\exists Z\geq 0 \text{ such that } \begin{cases} ZE_? = 0 \\ \rho_1\Sigma^{-1}(Z-\eta_1\rho_1)\Sigma^{-1}\rho_1=0 \\ \rho_0\Sigma^{-1}(Z-\eta_0\rho_0)\Sigma^{-1}\rho_0=0 \end{cases} \tag{82}$$

or in short

$$\exists Z\geq 0 \text{ such that } \begin{cases} ZE_? = 0 \\ \rho_i\Sigma^{-1}Z\Sigma^{-1}\rho_i=\eta_i\rho_i \text{ , for } i=0,1 \end{cases} \tag{83}$$

where we used Eqn. (74).

Third step

Since the operator Z is positive, we know there exists an operator Y such that $Z=YY^{\dagger}$. We can insert it in the relation $\rho_i\Sigma^{-1}Z\Sigma^{-1}\rho_i=\eta_i\rho_i$ and find, using the decomposition in Eqn.(1), that there exists a unitary transformation W_i such that

$$W_i^{\dagger}Y^{\dagger}\Sigma^{-1}\rho_i=\sqrt{\eta_i}\sqrt{\rho_i},\ \ i=0,1. \tag{84}$$

Moreover Σ is full rank since ρ_0 and ρ_1 span the total Hilbert space [14]. We can then decompose Z as $Z=\Sigma\Sigma^{-1}Z\Sigma^{-1}\Sigma=\rho_0\Sigma^{-1}Z\Sigma^{-1}\rho_0+\rho_0\Sigma^{-1}Z\Sigma^{-1}\rho_1+\rho_1\Sigma^{-1}Z\Sigma^{-1}\rho_0+\rho_1\Sigma^{-1}Z\Sigma^{-1}\rho_1$. This directly yields

$$\begin{aligned} Z &= \eta_0\rho_0+\eta_1\rho_1+\sqrt{\eta_0\eta_1}\sqrt{\rho_0}W_0^{\dagger}W_1\sqrt{\rho_1}+\sqrt{\eta_0\eta_1}\sqrt{\rho_1}W_1^{\dagger}W_0\sqrt{\rho_0} \\ &= (\sqrt{\eta_0}\sqrt{\rho_0}W_0^{\dagger}W_1+\sqrt{\eta_1}\sqrt{\rho_1})(\sqrt{\eta_0}W_1^{\dagger}W_0\sqrt{\rho_0}+\sqrt{\eta_1}\sqrt{\rho_1}) \end{aligned} \tag{85}$$

We finally read off $Y^{\dagger}$ as

$$Y^{\dagger}=\sqrt{\eta_0}W^{\dagger}\sqrt{\rho_0}+\sqrt{\eta_1}\sqrt{\rho_1} \tag{86}$$

where $W^{\dagger}=W_1^{\dagger}W_0$.

We now make use of the relation $ZE_?=0$ (Eqn.(64)) which is equivalent to $Y^{\dagger}E_?=0$. We can now explicitly write $Y^{\dagger}E_?=0$ with $Y^{\dagger}=\sqrt{\eta_0}W^{\dagger}\sqrt{\rho_0}+\sqrt{\eta_1}\sqrt{\rho_1}$ and $W=W_0^{\dagger}W_1$. Therefore the statement:

$$\exists Z\geq 0 \text{ such that } \begin{cases} ZE_? = 0 \\ \rho_i\Sigma^{-1}Z\Sigma^{-1}\rho_i=\eta_i\rho_i \text{ , for } i=0,1, \end{cases} \tag{87}$$

can be replaced by:

There exists a unitary transformation W such that

$$-\sqrt{\eta_0}W^{\dagger}\sqrt{\rho_0}E_?=\sqrt{\eta_1}\sqrt{\rho_1}E_?. \tag{88}$$

Note that this really is an equivalence and it is not difficult to go from (88) to (87). If a unitary W exists such that $-\sqrt{\eta_0}W^\dagger\sqrt{\rho_0}E_? = \sqrt{\eta_1}\sqrt{\rho_1}E_?$ then we can write $(\sqrt{\eta_0}W^\dagger\sqrt{\rho_0}+\sqrt{\eta_1}\sqrt{\rho_1})E_? = 0$ and define the operator $Z = YY^\dagger \geq 0$ with $Y^\dagger$ as $\sqrt{\eta_0}W^\dagger\sqrt{\rho_0}+\sqrt{\eta_1}\sqrt{\rho_1}$. We then immediately obtain that there exists a positive semi-definite operator Z such that $ZE_? = 0$. To recover Eqn.(87) it remains to check that $\rho_i\Sigma^{-1}Z\Sigma^{-1}\rho_i = \eta_i\rho_i$, for $i = 0, 1$, which can be easily done.

Eldar's conditions together with the assumptions that E_i $(i = 0, 1)$ have rank r_i and ρ_0 and ρ_1 have no overlapping supports are now extremely simplified. We shall now find the final equivalence in two more brief steps.

Fourth step
From Eldar's equations we notice that $\mathrm{Tr}(Z) = P^{opt}_{success}$. Indeed, $\mathrm{Tr}(Z) = \mathrm{Tr}(ZE_?) + \mathrm{Tr}(ZE_0) + \mathrm{Tr}(ZE_1) = \mathrm{Tr}(\sqrt{E_0}Z\sqrt{E_0}) + \mathrm{Tr}(\sqrt{E_1}Z\sqrt{E_1}) = \mathrm{Tr}(\sqrt{E_0}\eta_0\rho_0\sqrt{E_0}) + \mathrm{Tr}(\sqrt{E_1}\eta_1\rho_1\sqrt{E_1})$ where we used Eqns. (64), (65) and (66) . Therefore, with the form of Z we found in step 3, the optimal failure probability is given by

$$\begin{aligned} Q^{opt} &= -\sqrt{\eta_0\eta_1}(\mathrm{Tr}(\sqrt{\rho_0}W\sqrt{\rho_1}) + \mathrm{Tr}(\sqrt{\rho_1}W^\dagger\sqrt{\rho_0})) &(89)\\ &= 2\sqrt{\eta_0\eta_1}\mathrm{Re}[-\mathrm{Tr}(W^\dagger\sqrt{\rho_0}\sqrt{\rho_1})]. &(90)\end{aligned}$$

The fidelity can be expressed as $F = \max_U |\mathrm{Tr}(U^\dagger\sqrt{\rho_0}\sqrt{\rho_1})|$ where the maximum is taken over all the unitary transformations. This already implies that

$$Q^{opt} \leq 2\sqrt{\eta_0\eta_1}F. \tag{91}$$

But of course we know that[14]

$$Q^{opt} \geq 2\sqrt{\eta_0\eta_1}F. \tag{92}$$

Therefore $Q^{opt} = 2\sqrt{\eta_0\eta_1}F$[38].

Fifth step
The proof is almost done. Indeed we only need to see that

$$Q^{\mathrm{opt}} = 2\sqrt{\eta_0\eta_1}F \Leftrightarrow \begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1 \geq 0. \end{cases} \tag{93}$$

This equivalence has been already proved in [14] and we repeat here the corresponding theorem for convenience.

Theorem 3 *[14] Necessary and sufficient conditions to saturate the bounds on the failure probability*
Consider a USD problem defined by the two density matrices ρ_0 and ρ_1 and their respective a priori probabilities η_0 and η_1 such that their supports satisfy $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ (Any USD problem of two density matrices can be reduced to such a form according to [12]). Let F_0 and F_1 be the two operators $\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}$ and $\sqrt{\sqrt{\rho_1}\rho_0\sqrt{\rho_1}}$. The fidelity F of the two states ρ_0 and ρ_1 is then given by $F = Tr(F_0) = Tr(F_1)$. We denote by P_0 and P_1, the projectors onto the support of ρ_0 and ρ_1. The optimal failure probability Q^{opt} for USD then satisfies

$$Q^{\mathrm{opt}} = \eta_1\frac{F^2}{Tr(P_1\rho_0)} + \eta_0\, Tr(P_1\rho_0) \;\Leftrightarrow\; \begin{cases} \rho_0 - \frac{Tr(P_1\rho_0)}{F}F_0 \geq 0 \\ \rho_1 - \frac{F}{Tr(P_1\rho_0)}F_1 \geq 0 \end{cases} \text{ for } \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{Tr(P_1\rho_0)}{F} \tag{94}$$

$$Q^{\mathrm{opt}} = 2\sqrt{\eta_0\eta_1}F \;\Leftrightarrow\; \begin{cases} \rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0 \geq 0 \\ \rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1 \geq 0 \end{cases} \text{ for } \frac{Tr(P_1\rho_0)}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{F}{Tr(P_0\rho_1)} \tag{95}$$

$$Q^{\mathrm{opt}} = \eta_0\frac{F^2}{Tr(P_0\rho_1)} + \eta_1\, Tr(P_0\rho_1) \;\Leftrightarrow\; \begin{cases} \rho_0 - \frac{F}{Tr(P_0\rho_1)}F_0 \geq 0 \\ \rho_1 - \frac{Tr(P_0\rho_1)}{F}F_1 \geq 0 \end{cases} \text{ for } \frac{F}{Tr(P_0\rho_1)} \leq \sqrt{\frac{\eta_1}{\eta_0}} \tag{96}$$

This completes the proof. ■

Appendix B: Tighter bounds

It has been already shown in [14, 18] that the positivity of the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1$ is only possible when

$$\frac{\mathrm{Tr}(P_1\rho_0)}{F} \leq \sqrt{\frac{\eta_1}{\eta_0}} \leq \frac{F}{\mathrm{Tr}(P_0\rho_1)}. \tag{97}$$

These boundaries were built considering some very general constraints on Q_0 and Q_1 [14]:

$$\eta_0\mathrm{Tr}(P_1\rho_0) \leq Q_0 \leq \eta_0, \tag{98}$$
$$\eta_1\mathrm{Tr}(P_0\rho_1) \leq Q_1 \leq \eta_1, \tag{99}$$

where P_i denotes the projector onto the support of ρ_i, $i = 0, 1$. If more knowledge on the two density matrices ρ_0 and ρ_1 is provided, we can obtain stronger constraints on Q_0 and Q_1 and therefore tighter boundaries of the regime (97) (See details in [14]).
Let us give such an example of stronger constraints on Q_0 for, say, a POVM having the GU symmetry $E_1 = UE_0U$ where $U^2 = \mathbb{1}$. Since $E_0 \subset \mathcal{K}_{\rho_1}$, there exists $R \geq 0$ in $\mathcal{K}_{\rho_1}$ such that $P_1^\perp = E_0 + R$ and therefore $E_1 + E_? = P_1 + R$. Moreover the POVM element $E_?$ is invariant under U since $UE_?U = U(\mathbb{1} - E_0 - E_1)U = (\mathbb{1} - E_1 - E_0) = E_?$. Hence, $E_0 + E_? = U(E_1 + E_?)U = P_0 + URU$. We therefore derive the trace equality

$$\mathrm{Tr}(E_?) = 2\mathrm{Tr}(R). \tag{100}$$

Indeed $\mathrm{Tr}(E_1 + E_?) = \mathrm{Tr}(P_1) + \mathrm{Tr}(R)$ and $\mathrm{Tr}(E_0 + E_?) = \mathrm{Tr}(P_0) + \mathrm{Tr}(R)$ so that $\mathrm{Tr}(\mathbb{1}) + \mathrm{Tr}(E_?) = \mathrm{Tr}(P_0) + \mathrm{Tr}(P_1) + 2\mathrm{Tr}(R)$. And, for a USD problem in standart form, the equality $\mathrm{Tr}(\mathbb{1}) = \mathrm{Tr}(P_0) + \mathrm{Tr}(P_1)$ holds.

We can now consider Q_0. Since $E_1 + E_? = P_1 + R$ and $\mathrm{Tr}(E_1\rho_0) = 0$, we can write

$$\begin{aligned} Q_0 &= \eta_0\mathrm{Tr}(E_?\rho_0) && (101)\\ &= \eta_0\mathrm{Tr}(E_?\rho_0) + \eta_0\mathrm{Tr}(E_1\rho_0) && (102)\\ &= \eta_0\mathrm{Tr}(P_1\rho_0) + \eta_0\mathrm{Tr}(R\rho_0). && (103)\end{aligned}$$

The operator $P_1^\perp\rho_0P_1^\perp$ is positive semi-definite. We can here introduce λ_{min}, its smallest non vanishing eigenvalue. It follows that $Q_0 \geq \eta_0\mathrm{Tr}(P_1\rho_0) + \eta_0\mathrm{Tr}(R)\lambda_{min}$. Together with Eqn.(100) this yields

$$\begin{aligned} Q_0 &\geq \eta_0\mathrm{Tr}(P_1\rho_0) + \frac{\eta_0\lambda_{min}}{2}\mathrm{Tr}(E_?) && (104)\\ &\geq \eta_0\mathrm{Tr}(P_1\rho_0) + \frac{\eta_0\lambda_{min}}{2}\mathrm{Tr}(E_?\rho_0). && (105)\end{aligned}$$

In other words, for any USD POVM such that $E_1 = UE_0U$ where U is an involution,

$$\frac{\eta_0\mathrm{Tr}(P_1\rho_0)}{1 - \lambda_{min}/2} \leq Q_0 \tag{106}$$

where $\lambda_{min} = min\{Spect(P_1^\perp\rho_0P_1^\perp)\}$. It becomes clear that with more knowledge on the mixed states ρ_0 and ρ_1, we could make tighter the boundaries of the regime (97). The extreme case would be a regime reduced to a single value $\sqrt{\frac{\eta_1}{\eta_0}} = 1$. These considerations might indicate that, in general, E_0 and E_1 have rank E_0 and E_1, respectively, only for some regime of the ratio $\sqrt{\frac{\eta_1}{\eta_0}}$ around 1.

Appendix C: Proof of Corollary 1

To prove this corollary we begin with the statement given in Theorem 1 for two density matrices ρ_0 and ρ_1 with the same rank r in a $2r$-dimensional Hilbert space. If the two operators $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1$ are not positive semi-definite Theorem 1 tells us that at least one of the two POVM elements E_0 and E_1 has rank strictly smaller than r. Without loss of generality we say that $r_{E_0} < r$. Because of the completeness relation $E_? + E_1 + E_0 = \mathbb{1}$ fulfilled by

the POVM elements we have on the support $\mathcal{S}_{\rho_0}$ the equality $P_0E_?P_0 + P_0E_1P_0 + P_0E_0P_0 = P_0$. However $\mathcal{S}_{E_1} \in \mathcal{K}_{\rho_0}$ so that we are left with

$$P_0E_?P_0 + P_0E_0P_0 = P_0. \tag{107}$$

Furthermore we can consider the spectral decomposition of the hermitian operator $P_0E_0P_0$ and write

$$P_0E_0P_0 = \sum_{i=1}^{r-1} \lambda_i |\lambda_i\rangle\langle\lambda_i| \tag{108}$$

$$P_0 = \sum_{i=1}^{r-1} |\lambda_i\rangle\langle\lambda_i| + |e\rangle\langle e| \tag{109}$$

where $|e\rangle$ completes the r dimensional orthogonal basis of $\mathcal{S}_{\rho_0}$. As a result $E_?|e\rangle = (\mathbb{1} - E_0 - E_1)|e\rangle = |e\rangle - 0 - 0$ and $|e\rangle$ is an eigenvector of $E_?$ with eigenvalue 1. Moreover since $|e\rangle$ is eigenvector with eigenvalue 1 the completeness relation is already fulfilled onto the subspace spanned by $|e\rangle$. Therefore no optimization is required onto that subspace and we can split it off from the original USD problem. If we denote by $\mathcal{S}_{|e\rangle}$ the subspace of $\mathcal{S}_{\rho_0}$ spanned by $|e\rangle$, the reduced Hilbert space is $\mathcal{H}/\mathcal{S}_{|e\rangle}$ and the support $\mathcal{S}_{\rho_0}$ looses one dimension. The remaining USD problem to optimize concerns ρ_0' and ρ_1' originated from the density matrix ρ_0 and ρ_1. Here ρ_0' has rank $r-1$ while ρ_1' has rank r. Thanks to the second reduction theorem, we can reduce this problem to the one of two density matrices of rank $r-1$ in a Hilbert space of dimension $2r-2$. Indeed, the subspace $\mathcal{K}_{\rho_0'} \cap \mathcal{S}_{\rho_1'}$ is one dimensional and leads to the detection of ρ_1' with unit probability [12]. We call $|e'\rangle$ the unit vector spanning this one dimensional subspace. We are left with a reduced USD problem in a $2r-2$ dimensional Hilbert space. Importantly, $|e'\rangle$ is in $\mathcal{K}_{\rho_0'} \cap \mathcal{S}_{\rho_1'} \subset \mathcal{K}_{\rho_0'} = \mathcal{K}_{\rho_0}$. Indeed, $\mathcal{H} = \mathcal{S}_{\rho_0} \oplus \mathcal{K}_{\rho_0} = \mathcal{S}_{\rho_0'} \oplus \mathcal{S}_{|e\rangle} \oplus \mathcal{K}_{\rho_0}$ so that, in $\mathcal{H}' = \mathcal{H}/\mathcal{S}_{|e\rangle}$, $\mathcal{K}_{\rho_0'} = \mathcal{K}_{\rho_0}$.
In other words if $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1$ are not positive then there exists $|e\rangle$ in $\mathcal{S}_{\rho_0}$, eigenvector of $E_?$ with eigenvalue 1, and $|e'\rangle$ in $\mathcal{K}_{\rho_0}$, eigenvector of E_1 with eigenvalue 1. Without the assumption $r_{E_0} < r_0$ we have the general statement that if $\rho_0 - \sqrt{\frac{\eta_1}{\eta_0}}F_0$ and $\rho_1 - \sqrt{\frac{\eta_0}{\eta_1}}F_1$ are not positive then there exists $|e\rangle$ in either $\mathcal{S}_{\rho_0}$ or $\mathcal{S}_{\rho_1}$, eigenvector of $E_?$ with eigenvalue 1 and $|e'\rangle$ either in $\mathcal{K}_{\rho_0}$ and eigenvector of E_1 with eigenvalue 1, or in $\mathcal{K}_{\rho_1}$ and eigenvector of E_0 with eigenvalue 1. The completes the proof. ■

---

[1] D. Dieks, Phys. Lett. A **126**, 303 (1988).
[2] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[3] A. Peres, Phys. Lett. A **128**, 19 (1988).
[4] G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).
[5] A. Chefles, Phys. Lett. A **239**, 339 (1998).
[6] A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).
[7] X. M. Sun, S. Y. Zhang, Y. Feng, and M. S. Ying, Phys. Rev. A **65**, 044306 (2002).
[8] L. Vandenberghe and S. Boyd, SIAM Review **38**, 49 (1996).
[9] L. Vandenberghe and S. Boyd, *Convex Optimization* (Cambridge University Press, 2004).
[10] A. Ben-Tal and A. Nemirovski, *Lectures on Modern Convex Optimization* (MPS/SIAM Series on Optimization, Philadelphia, 2001).
[11] Y. Eldar, IEEE Trans.Inf. Theory **49**, 446 (2003).
[12] P. Raynal, N. Lütkenhaus, and S. van Enk, Phys. Rev. A **68**, 022308 (2003).
[13] P. Raynal, PhD thesis, quant-ph/0611133 (2006).
[14] P. Raynal and N. Lütkenhaus, Phys. Rev. A **72**, 022342 (2005).
[15] T. Rudolph, R. W. Spekkens, and P. S. Turner, Phys. Rev. A **68**, 010301(R) (2003).
[16] S. Barnett, A. Chefles, and I. Jex, Phys. Lett. A **307**, 189 (2003).
[17] M. Kleinmann, H. Kampermann, and D. Bruss, Phys. Rev. A **72**, 032308 (2005).
[18] U. Herzog and J. Bergou, Phys. Rev. A **71**, 050301(R) (2005).
[19] Y. Sun, J. A. Bergou, and M. Hillery, Phys. Rev. A **66**, 032315 (2002).
[20] J. A. Bergou, U. Herzog, and M. Hillery, Phys. Rev. Lett. **90**, 257901 (2003).
[21] J. Bergou, U. Herzog, and M. Hillery, Phys. Rev. A **71**, 042314 (2005).
[22] J. A. Bergou, E. Feldman, and M. Hillery, Phys. Rev. A **73**, 032107 (2006).
[23] Y. C. Eldar, M. Stojnic, and B. Hassabi, Phys. Rev. A **69**, 062318 (2004).
[24] X.-F. Zhou, Y.-S. Zhang, and G. Guo, quanth-ph/0611095 (2006).

[25] C. W. Helstrom, *Quantum detection and estimation theory* (Academic Press, New York, 1976).
[26] Y. Eldar and G. Forney, IEEE Trans. Inf. Theory **47(3)**, 858 (2001).
[27] Y. Eldar, A. Megretski, and G. Verghese, quant-ph/0211111 (2002).
[28] Y. C. Eldar, Phys. Rev. A **67**, 042309 (2003).
[29] Y. Eldar and H. Bolcskei, IEEE Trans. Inf. Theory **49**, 993 (2003).
[30] U. Herzog, quanth-ph/0611087 (2006).
[31] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[32] M. Dušek, M. Jahma, and N. Lütkenhaus, Phys. Rev. A **62**, 022306 (2000).
[33] In the case of a standard form, we not only have $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ but also $\mathcal{K}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ and $\mathcal{K}_{\rho_1} \cap \mathcal{S}_{\rho_0} = \{0\}$.
[34] In a cryptographic context, the *bit value* states and *basis* states in the BB84-type protocol using weak coherent pulses and a phase reference exhibit such a GU symmetry.
[35] Let us note that this result would be immediately extended to any pair of unitary equivalent mixed states as soon as the statement in [23] would be extended to unitary equivalent mixed states.
[36] The implication from the right to the left is the only important direction for our purpose. The assumption $\mathcal{S}_{\rho_0} \cap \mathcal{S}_{\rho_1} = \{0\}$ is required to prove that if $\rho_0 - F_0 \geq 0$ then $Q^{\text{opt}} = F$. Without this assumption, only the other direction is true (See [14] for more details).
[37] In [32], the four signal states are two modes signal states where the first mode carries the phase reference. Moreover in [32] the complex amplitude α is multiplied by a factor $\frac{1}{\sqrt{2}}$. This is due to the technique used to implement the polarized coherent states. To simplify the analysis here, we simply omit the first mode and the multiplicative factor.
[38] Note that we can even conclude that $-W$ comes from a polar decomposition of $\sqrt{\rho_0}\sqrt{\rho_1}$ since $-\text{Tr}(W^\dagger \sqrt{\rho_0}\sqrt{\rho_1})$ equals F.